Security Exceptions and Exemptions to ITS Security Controls Request Form

This form is used to request an exception or exemption to established UTHSC Information Technology and Office of Cybersecurity Policies and Standards. An exception is a request considered to be short-term while an exemption would be considered long-term or permanent. Exceptions/exemptions should be reviewed or renewed annually if they represent very low to medium risk or every six months if they are high risk or above. Carefully evaluate the potential impact on operations, as well as the impact on the security, privacy, and legal posture of the system, unit, UTHSC and the University of Tennessee before submitting this request.

Section 1 – System/Data Owner

Identify the Requestor and the Authorized Signer according to Practice-InfoSec-RA-001.01-Risk Assessment Process in Figure 8. The Authorized Signer will be responsible for privacy and security incidents that may occur because of the exception/exemption.

Requestor's Name: _____

Requestor's Contact Phone #: _____

Requestor's Contact Email Address: _____

Name of Business Unit or College: _____

Name of Authorized Signer: _____

Section 2 – Description of the Request

Fill in the required fields to describe the control, standard or practice the exception is requested as well as explain the need for the exception. Describe the rationale for the exception, plus any applicable mitigation of the risk involved with the exception.

Name of the security control, standard or practice: _____

Request Type (based on definitions found in InfoSec-GP-001.02 Security Exceptions and Exemptions to ITS Standards and Practices):

☐ Exception (Short Term or Temporary Request)
☐ Exemption (Long Term or Permanent Request)

Explanation of the Request:

```
┌─────────────────────────────────────────────────────┐
│                                                       │
│                                                       │
│                                                       │
│                                                       │
└─────────────────────────────────────────────────────┘
```

Business Justification/Reason:

```
┌─────────────────────────────────────────────────────┐
│                                                       │
│                                                       │
│                                                       │
│                                                       │
└─────────────────────────────────────────────────────┘
```

Explanation of Risk to be Accepted (risk analysis):

Risk Mitigation Plan/Explanation of Mechanisms for Compliance (if applicable)

Section 3 – Approval or Rejection

The Authorized Signer must review the request and provide definitive approval or rejection of the request.

I,_____:
        Authorized Signer

☐ Approve the request for exception with the understanding the business unit/University assumes the associated risks and ensures that alternative countermeasures are implemented

☐ Reject this request for exception with an explanation below.

Reason for rejection:

Section 4 – Office of Cybersecurity Acknowledgment and Review

The Office of Cybersecurity must review the form and document the exception/exemption in the Risk Register with the appropriate dates for review per Practice-InfoSec-RA-001.01-Risk Assessment Process.

_____   _____
        Cybersecurity Analyst   Date